

INFORMATION APPLIANCE AND USE OF SAME IN DISTRIBUTED PRODUCTIVITY ENVIRONMENTS

CROSS REFERENCE TO RELATED APPLICATIONS

5 This application claims the benefit of U.S. Provisional Application No. 60/241,523
filed October 18, 2000, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

10 The present invention relates in general to information appliances, and in
particular to systems and methods for adding or removing programs and data to the
information appliance without having to reprogram the file or data structure therein.
The present invention further relates to the secure implementation of such information
appliances in distributed productivity environments.

15 Information appliances are playing an ever increasing role in the day-to-day
transactions of commercial and consumer activities. For example, information
appliances in the form of smart cards are appearing more common in the debit and
credit industries. Personal digital assistants (PDA's), cell phones, and other hand held
portable devices now offer access to the Internet to send and retrieve messages,
20 perform financial and other transactions, and store and retrieve data. Also, information
appliances embedded in form factor items such as refrigerators and ovens are
becoming more readily available that communicate over the Internet to place their own
service calls, download recipes, and perform other intelligent functions.

25 In current practice, information contexts including data, programs, and other
information are stored on information appliances and other binary devices as a
sequence of bits. For organizational and other reasons, each particular information
context is stored as a discrete file. As such, a given device manages multiple
information contexts by managing a number of discrete files.

Typically, the necessary files are programmed into information appliances prior to distribution of the information appliance to the intended recipient. However, it often occurs that new applications, features, or functions are desired to be added after an information appliance has been distributed. In order to implement the new and
5 desirous changes, the file structure of the information appliance must be modified or reprogrammed. This modification frequently requires that all information appliances in the field are recalled and replaced with new versions containing the additional functionality. Unfortunately, recall and reissue campaigns are time consuming and costly.

10
15
20
25
In addition to the technical challenge of implementing file structures on information appliances, consumer confidence in using the product must be earned. That is, in order for information appliances to gain wide acceptance, users must believe that the information being exchanged through the information appliance is accurate, secure, and transacted between legitimate parties. Therefore, identification, authentication, security, and information validity issues must be addressed in electronic transaction systems that incorporate information appliances. For example, in telemedicine and telehealth applications, there is a strong need to protect the substance and character of transactions between the patient and care-provider. These
issues are important for patient-care-giver trust and, in some cases, may be subject to regulatory environments including the uniform reporting requirements of HIPAA. Because of the remote access character of such processes, technologies and processes are needed to positively identify and authenticate the patient and health-care individuals involved in telemedicine and telehealth transactions. The need for security,
authentication and identification are not limited to telemedicine and telehealth applications. Rather, there are a number of existing and emerging applications that require security, authentication, and identification.

Accordingly, there is a need for systems and methods of storing programs and
30 information on information appliances including smart cards, that eliminates the need

for an independent file structure for each individual information context. Further, there is a need for an information appliance that allows new programs and information to be added, and existing programs or data to be edited or subtracted without having to reprogram the structure on the information appliance. Still additionally, there is a need
5 for an information appliance that can transact securely in a distributed productivity environment, and that provides a convenient and effective manner of identifying and authenticating users.

SUMMARY OF THE INVENTION

10 The present invention overcomes the disadvantages of previously known information appliances by organizing individual information contexts as segments within a single linear sequence or string where the different segments are delimited by known bit patterns or by different encoded representations. Each segment may include for example, information contexts intended for different applications. Accordingly, the
15 information appliance is required to manage only a single string for all information contexts used thereby, regardless of the number of information contexts including applications and data stored therein. The storage of multiple and discrete data and programs as segments within a single file provides a highly portable system useful in the exchange of information between information appliances, such as smart cards,
20 remotely, through the Internet. In this configuration, the implementation of reading from and writing to the string can be carried out within the information appliance itself, by a client application operating between the information appliance and a network such as the Internet, or by a remote host performing data exchange with the information appliance over the network.

25 In applications involving distributed productivity environments utilizing the Internet or other network, the present invention is also useful in accomplishing security, authentication and identification tasks. In these applications, biometric or other security data including secret/personal information such as passcodes, personal identification
30 numbers, and certificates are stored in the string. The security data is accessible by

applications to verify the authenticity of the identified user. Further, encryption methods using symmetric and asymmetric keys provide a mechanism for securing data stored on the information appliance.

5 Accordingly, it is an object of the present invention to provide systems and methods of storing programs and information on information appliances including smart cards that eliminates the need for an independent file structure for each individual information context.

10 It is an object of the present invention to provide an information appliance that allows new programs and information to be added, and existing programs or data to be edited or subtracted from the system without having to reprogram the structure on the information appliance.

15 It is an object of the present invention to provide an information appliance that can transact securely in a distributed productivity environment, and that provides a convenient and effective manner of identifying and authenticating users.

20 Other objects of the present invention will be apparent in light of the description of the invention embodied herein.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

25 The following detailed description of the preferred embodiments of the present invention can be best understood when read in conjunction with the following drawings, where like structure is indicated with like reference numerals, and in which:

30 Fig. 1 is a schematic illustration of a structure for storing different information contexts as delimited segments in a single string according to one embodiment of the present invention;

Fig. 2 is a schematic illustration of the structure of Fig.1, where a select one of the segments is removed from the string, processed, then returned to the string in the same relative position, according to one embodiment of the present invention;

5 Fig. 3 is a schematic illustration of a structure for storing different information contexts as delimited segments in a single string where each delimiter is unique according to another embodiment of the present invention;

10 Fig. 4 is a schematic illustration of the structure of Fig. 3, where a select one of the segments is removed from the string, processed, then returned to the string by appending the removed segment to the end of the string;

15 Fig. 5 is a flow diagram illustrating a typical operation where the contents of the string are read but not changed according to one embodiment of the present invention;

20 Fig. 6 is a flow diagram illustrating a typical read, process, and write operation according to one embodiment of the present invention;

25 Fig. 7 is a schematic illustration of a first encrypting scheme according to one embodiment of the present invention, where a unique encryption process encrypts each segment of the string separately;

Fig. 8 is a schematic illustration of a typical decryption process for decrypting the encrypted string of Fig. 7 according to one embodiment of the present invention;

Fig. 9 is a schematic illustration of a typical encryption and decryption process according to another embodiment of the present invention;

Fig. 10 is an illustration of an information appliance implemented as a smart card connectable to a distributed productivity environment according to one embodiment of the present invention; and,

5 Fig. 11 is an illustration of a plurality of information appliances communicating across a distributed productivity environment according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

10 In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration, and not by way of limitation, specific preferred embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and that logical changes may be made without departing from the spirit and scope of the present invention.

The Information Appliance:

15 The present invention is directed to information appliances and the use of information appliances across distributed productivity environments. Information appliances can be embodied in a number of forms ranging from simple memory devices to computer-controlled devices. For example, information appliances may include contact and contactless smart cards including memory and microprocessor based smart cards, secure portable tokens, hand held devices such as Personal Digital Assistants (PDA), internet phones, electronics integrated into established form factor items such as VCRs, televisions, and kitchen appliances, intelligent sensors, actuators, 20 RFID devices, any digital electronics that provide consumer-focused access to the features and benefits of the Internet, and other formatted binary storage devices.

Information Appliance File Structure:

One aspect of the present invention comprises methods and techniques for loading and storing programs and data on information appliances. In a typical information appliance, each distinct information context is stored as a separate file.

5 Each file comprises a collection of related data, program, records, or other information stored as a unit with a single name. A file can include any number of different file types including for example, data files, text files, program files, and directory files. However, the present invention provides a unique file structure wherein data and programs for multiple and diverse applications are stored on information appliances as a single delimited string.

10 Referring generally to Figs. 1 through 11, various exemplary techniques are illustrated for storing information including data and programs on an information appliance such that multiple applications can be saved as a single string. This unique approach to storing data facilitates the selective performance one or more different applications. More particularly, data and applications can be added, removed, or edited without the need to reprogram the information appliance.

15 Referring to Fig. 1, a single string 10 is stored in a memory area of an information appliance. The string 10 is comprised of a plurality of segments 12, 14, 16, and 18. As shown, segment 12 comprises information context "A", segment 14 comprises information context "B", segment 16 comprises information context "C", and segment 18 comprises information context "D". The segments 12, 14, 16, and 18 are data, programs, or other information, intended for use by different applications. For
20 example, segment 12 may comprise biometric information for an authentication program. Segment 14 may comprise data used by an epurse program. Segment 16 may comprise information and data for a credit provider's application, and segment 18 may comprise program for performing certain administrative functions. As such, the type of stored information will depend upon the nature of the application to which the
25

segment is associated. Interleaved between each of the segments 12, 14, 16, 18 are delimiters or segment identifier 20 (represented by the symbol K).

The segment identifiers 20 are known bit patterns or encoded representations that provide bounds to the individual segments 12, 14, 16, and 18. In this manner, a specific segment containing programs or data for a particular application or function of the information appliance can be recovered and accessed through the detection and removal of the segment identifiers 20. It will be appreciated that each of the segments 12, 14, 16, and 18 are stored as separate files in conventional practice. In contrast, according to the present invention, a single string is comprised of one or more delimited segments where each of the delimited segments comprises a delimiter or segment identifier 20, and a segment. It will be appreciated that the number of segments in a given string 10 can vary depending upon the number of different applications to be accommodated by the information appliance. Further, the string 10 may be embodied in a number of ways including for example, a linear sequence, file or string.

An example of a technique for recovering a predetermined one of the segments 12, 14, 16, and 18 is illustrated in Fig. 2. To recover information context B stored in segment 14, the string 10 is serially read out, and the delimiting patterns K of the segment identifiers 20 are detected and removed until segment 14 (information B) is recovered. As illustrated, the segment identifiers 20 are identical (represented as delimiting pattern K) throughout the string 10. Accordingly, to recover the segment 14, the position of the segment 14 within the string 10 must be known. Once recovered, the segment 14 is processed as required by its associated application 22. If segment 14 is to be removed from the information appliance, the string is saved back to the information appliance without segment 14.

To store the edited information B' back to the information appliance, the segment 14 containing edited information B' must be returned to the same position within the

string 10 such that the order of the segments is preserved. Likewise, the associated application 22 may be used to add a new segment. As shown, the original string 10 comprises segments 12, 14, 16. To add a new segment 18, the segment 18 is concatenated with a segment identifier 20 and is appended to the end of the string 10.

- 5 The relative position of the new segment 18 within the string 10 is recorded, and the string is written back to the information appliance.

Referring to Fig. 3, another embodiment of the present invention is illustrated where each segment identifier 20 in the string 10 has a unique delimiting bit pattern. As such, the serial access methods described above with reference to Fig. 2 may optionally be replaced with random access methods. For example, the segment identifier 20 that precedes segment 14 contains the unique delimiting pattern K2. Referring to Fig. 4, to recover the segment 14, the string 10 is searched for the segment identifier 20 containing the delimiting bit pattern K2. The segment identifier 20 containing delimiting bit pattern K2 is stripped off, and information context B contained in segment 14 is read out. The information context B is manipulated by its associated application 22, rendering information context B'. The segment identifier 20 containing the delimiting bit pattern K2 is then written back out along with segment 14 (containing new information context B'). Because the segment identifier 20 is written out with the segment 14, the exact positioning of the segment 14 within the string 10 need not be preserved. For example, as illustrated, the segment 14 is moved to the end of the string 10.

According to one embodiment of the present invention, the length of each segment 12, 14, 16, and 18 is recorded in the string. This allows the information appliance to recover the entire segment after locating a single segment identifier 20. Under this arrangement, the desired segment identifier 20 (predetermined delimiter) is located within the string 10. Next, the segment length is read out to determine the length of the desired or predetermined segment. For example, the segment length is

encoded in one or more bytes in a first portion adjacent to the predetermined delimiter. Subsequently, the segment is read out.

In certain applications, a select one of the segments 12, 14, 16, and 18 is read but not altered. For example, in certain biometric applications, data from a reader such as a finger print reader is compared to predetermined finger print data. Under this arrangement, no data will be written to the string 10. Referring to Fig. 5, a typical read operation flow 100 is illustrated. The segment identifier that corresponds to the segment of interest is chosen (see 102). The string is then searched to locate the requested segment identifier within the string (see 104). Once the segment has been located, the segment length is extracted (see 106). For example, the segment length can be stored as the first byte or bytes immediately following the segment identifier. Based upon the known segment length, the segment is then read out of the string (see 108) and the application associated with the recovered segment processes the segment as the application dictates (see 110).

Referring to Fig. 6, a typical operation involving a string read and write cycle is illustrated. The segment identifier that corresponds to the segment of interest is selected (see 122). The string is then searched to locate the requested segment identifier within the string (see 124). Once the segment has been located, the segment length is extracted (see 126). Based upon the known segment length, the segment is then removed from the string (see 128). Further, the segment identifier is stripped out. The string is then joined together (see 130) without the removed segment and segment identifier. The requesting application processes the segment (see 132). The processing of the segment can involve editing the segment contents, making additions and/or deletions. When the application has completed processing the segment, the new length of the segment is determined (see 134). The segment identifier, the determined length of the segment, and the segment are then concatenated (see 136) and reunited with the string (see 138). As discussed more thoroughly above,

depending upon the implementation of the segment identifiers, the edited data portion may be placed back in the same relative position from which it came, it can be appended either to the beginning or end of the string, or rejoined to the string after any segment.

5

The ability to concatenate segment identifiers and segments to the string further allows the addition of new delimiters and segments, and the removal of old or unused segment identifiers and segments from the string. For example, an upgrade application can engage in a transactional session with an information appliance to remove old segments and their associated segment identifiers, and new segments and associated segment identifiers that did not exist previously can be added to the string, by appending the new segments to the end of the string. These transactions may be accomplished in the background either with or without the customer's knowledge.

10

15

It will be appreciated that other techniques can be used within the present invention. For example, the information appliance can access a select one of the segments by locating a first delimiter and reading until a second delimiter is encountered. Under such a construction, the string need not include each segments length. Further, the exact implementation of the string will depend upon factors such as the information appliance operating system. For example, the flexible structure of the present invention allows the string, or linear sequence of delimited segments to be dropped into a file structure in the case of MPCOS and MULTOS, an object structure in the case of JAVA. Further, the string is easily adapted to other device operating systems, or any other storage format implemented by the information appliance.

20

25

Where security is an issue, the various embodiments of the present invention may be practiced with encryption techniques, including for example, the use of symmetric and asymmetric keys. Referring to Fig. 7, a security scheme according to one embodiment of the present invention is illustrated. Segment 12 containing

information context A is encoded using encryption routine 32. The encryption routine 32 is unique to the segment 12 and encrypts information context A to unintelligible information Z. Information context B in segment 14 is encoded by encryption routine 34 to render unintelligible information Y. Information context C in segment 16 is encoded by encryption routine 36 to render unintelligible information X. Information context D in segment 18 is encoded by encryption routine 38 to render unintelligible information W. The string 10 is then formed such that the segments 12, 14, 16, and 18 are stored as encoded unintelligible information Z, Y, X, and W, and is unintelligible if read. Because each segment 12, 14, 16, and 18 is encoded with a unique encryption routine 32, 34, 36, and 38, any single decoder will be unable to render multiple segments intelligible.

For example, referring to Fig. 8, where an application requires information from segment 14, a decryption routine 44 is used to process the string 10. The decryption routine 44 must be complimentary or otherwise compatible with the encryption routine 34 in order to render the segment 14 intelligible. The segment 12 containing information context A was encoded using encryption routine 32, which is not compatible with the decryption routine 44, thus segment 12 is decrypted to unintelligible information M. Because the decryption routine 44 is compatible with the encryption routine 34, the segment is successfully decrypted from encoded unintelligible information Y to the correct information context B. Segment 16 is decoded by the decryption routine 44 as unintelligible information O, and segment 18 is decoded by the decryption routine 44 as unintelligible information P. It will be appreciated that the serial or random access methods discussed above, using the same or unique bit patterns for the segment identifiers 20 may be practiced with this embodiment of the present invention to locate segment 14 after decrypting the string 10.

Referring to Fig. 9, a system using asymmetric keys according to one embodiment of the present invention is illustrated. Asymmetric keys are comprised of a key pair, including a first key and a second key. The first and second keys perform

inverse functions such that a message encrypted by the first key can be decrypted by the second key, and vice-versa. The entire information file 10 is encrypted using a private key or first key 50 and stored within the information appliance (Not shown in Fig. 9) in an encoded fashion. As illustrated, information context A is encoded to
5 unintelligible information Z, information context B is encoded to unintelligible information Y, information context C is encoded to unintelligible information X, and information context D is encoded to unintelligible information W. Assume an application or information appliance function requires the contents of segment 14. That application or function is provided with a public key or second key 54 that is capable of deciphering
10 only that data contained within the segment 14. As such, decoding the application file 10 with the public key 54 yields unintelligible information M in the segment 12, the proper information context B in the segment 14, unintelligible information O in the segment C, and unintelligible information P in the segment 18. It will be appreciated that the serial or random access methods discussed above, using the same or unique bit patterns for the segment identifiers 20 may be practiced with this embodiment of the
15 present invention to recover segment 14. Further, the roles of the private and public keys may be reversed, and alternatively, other encryption schemes may be used, including for example, symmetric key encryption.

20 A number of different security schemes may be implemented with the various embodiments of the present invention. This is especially true where the information appliance comprises a central processing unit. For example, the processor may be programmed to prevent data writes and reads unless some access parameter is achieved. According to one embodiment of the present invention, the information
25 appliance comprises a session key. The session key is used to manage the threat of disclosure by hacking of an individual smart appliance. Basically, the string or linear sequence containing the delimited segments is encrypted using a one-time session key. The one-time session key is separately encrypted and stored in an accessible location,

either within the information appliance, or a separate computer, and is used to unencrypt the string for processing.

It will be appreciated that while symmetric and asymmetric encoding are preferable, other forms of data security and encryption may be used. The application and security needs dictate the appropriate encryption schemes. According to one embodiment, a random seed is regenerated for each session writing to the information appliance. As such, a potential fraud perpetrator that gains access to the session key only potentially exposes the current content of the segments within the string 10, and not a subsequently encoded string 10.

Further, additional safeguards can be built into the smart appliance system to ensure that the content of segments are not corrupted. For example, redundant verification of the segments can be used to determine errors in returning the string. According to one embodiment of the present invention, redundant verification of the segment length is implemented. Further, appending edited segments to the end of the string instead of reinserting them back into their original location is known to reduce the chance of error when saving the string back to the information appliance.

It will further be appreciated that the present invention, including the above-described examples is portable, and can be applied to virtually any information appliance. The present invention is further advantageous in that an identification and authentication architecture is provided that does not rely on any proprietary or customized hardware devices. Further, because of the self-organizing arrangement of this data string, the string can be stored and retrieved over one or multiple files in order to accommodate its size. This characteristic allows the method to be used with any smart card storage scheme independent of the vendor.

Distributed Productivity Environments:

Information appliances according to the present invention, can be effectively leveraged in distributed productivity environments. Some information appliances such as those integrated with form factor devices including for example, web televisions, refrigerators and other household appliances may have an interface built in. However, generally, for portable information appliances such as smart cards, an appropriate reader or interface is required. The reader optionally supplies power to the information appliance, and provides an interface through which the information appliance can transact with other processes. The type of interface or reader will depend upon the embodiment of the information appliance, and thus will be generally referred to herein as peripheral interface device.

Referring to Fig. 10, a distributed system 200 comprises an information appliance 202, a smart card as illustrated, that is insertable into a peripheral interface device 204. The peripheral interface device 204 comprises a smart card reader, however, the type of peripheral interface device used, if one is even required, will depend upon the type of information appliance being interface. The peripheral interface device 204 communicates over a first communications link 206 to a first computer 208. The first communications link may comprise a direct cable connection, a network connection, a wired or wireless connection, or any other communications link. For example, the peripheral interface 204 may have a built in modem, network interface or other communications interface that allows communication between the information appliance 202 and the first computer 208 over any network, including for example, the Internet. The first computer 208 may comprise a personal computer, network computer, World Wide Web server, or any other computer, depending upon the intended application.

According to one embodiment of the present invention, the first computer 208 comprises a personal computer that communicates over a second communications link

210 to a second computer 212. The second communications link can be any wired or wireless connection to the Internet. The second computer 212 is comprises a server running Internet enabled software. Under this arrangement, processing of information stored on the information appliance 202 including cryptographic, authenticating and identifying tasks can be carried out on the information appliance itself, on the first computer 208, on the second computer or server 212, or any combination thereof. This flexibility allows the information appliance 202 to be compatible with virtual private networks, third party certificates, and other network security schemes, and additionally allows the information appliance to work with electronic commerce applications such as the Electronic Data Interchange platform. Preferably, the information appliance interfaces with a web browser running on the first computer 208, and the web browser on the first computer 208 communicates with web enabled applications on the server or second computer 212.

Information Appliance Security Systems:

Referring to Fig. 11, a secure transaction system 300 is arranged to provide secure and unambiguous information appliance transactions. To initiate a secure transaction, at least one information appliance forms a networked connection. For example, portable information appliances 301 such as the personal digital assistant or wireless hand set may have a built wired or wireless interface that allows a network connection to be established. An information appliance in the form of a smart card 302 is inserted into an appropriately configured peripheral device interface or smart card reader 304. The peripheral interface device 304 allows the information appliance 302 to communicate with a personal computer 306. The various devices including the personal computer 306 and portable information appliance 301 communicate over a network connection 308 to a server 310. The server 310 is arranged to confirm the

identity of a party logged into the server 310 by validating information obtained from the information appliance.

The information appliances 301, 302 utilize a file structure comprising a string of delimited segments according to the present invention. At least one segment of the string is configured to store identifying information. For example, one or more segments may contain biometric information such as data relating to a fingerprint, eye scan, face recognition, voice pattern, DNA sequence, or any other biometric feature.

Each computer 306 is further coupled to a biometrics interface device 312. The biometrics interface device 312 is arranged to read biometric information from the user.

The system 300 reads biometric information from the biometrics interface device 312 and compares that data to biometric data stored within the information appliance 302. Under this arrangement, the information appliance 302 actually verifies the identity of the user. Once the identity of the user is verified by the information appliance 302, the information appliance 302 can communicate with the computer 306 and the server 310.

Further, because a verified user has been properly authenticated, a coded, ambiguous, or otherwise disguised identity can be used in communications across the network to protect the privacy of the user. Accordingly, the user maintains possession and control over their own identifying and personal information, and that information is not broadcasted over any network.

As an alternative to biometric information, authenticating information may be stored on the information appliance in the form of a code such as personal identification number (PIN). In this case, a separate biometrics interface device 312 is not necessary. Rather, the user can enter their PIN in on a keyboard or other input/output device. Alternatively, a password or other similar passcode may be used to identify the user. For example, the portable information appliance 301 implemented as a PDA or

Internet phone already includes a simple keypad. As such, the identity of the user can be determined by requiring a user to enter an appropriate passcode.

Other security measures may be integrated into the secure transaction system 300 to provide authentication that the portable information appliance 301, 302 being used is not counterfeit. This is accomplished through asymmetric cryptographic key/message exchanges and verifications between the various wired and wireless networks and the portable information appliances 301, 302. For example, the string stored on the portable information appliance 301, 302 can be encrypted using any encryption techniques, including those described more fully herein. In a preferable security scheme, strings stored on each of the portable information appliances 301, 302 are encoded using a private key held by the server 310. A unique public key 316, 318, 320 is then provided to each user.

Further, various certificate schemes may be used. For example, ISO X.509 compliant digital certificates can be issued to each of the portable information appliances 301, 302. Under this arrangement, a certificate issuer provides encrypted delivery of an encryption key belonging to one of the transaction organizations. Inherent in the delivery is the authentication through the certifying organization of the identity of the key's owner.

By a providing encryption schemes, identifying the individuals through the portable information appliance directly through biometric and/or other secret personal information, and by having the portable information appliance 301, 302 identify the user, a secure information and/or transaction system is realized. It will be observed that the identity of the user is kept in the possession and control of the individual and not broadcast throughout the network. In this way, individual privacy concerns can be implemented in that the act of using the portable information appliance 301, 302 for

identification explicitly provides the individual's permission to perform identification activities.

It will be observed that this secure transaction system can be applied to any number of applications where privacy and security are concerns. For example, among telemedicine and telehealth implementation issues are those that address the protection and character of transactions between the patient and care-provider. These issues are important for patient-care-giver trust and, in some cases, may be subject to regulatory environments including the uniform reporting requirements of HIPAA. Because of the remote access character of telemedicine processes, technologies and processes are needed to positively identify and authenticate the patient and health-care individuals involved in telemedicine transactions.

The present invention can be used to positively identify remotely located individuals engaged in telemedicine/telehealth activities so as to assure patient-doctor confidential transactions. The authentication processes are used to prevent counterfeiting of the credentials of the patient or caregiver over remote distances while engaged in telemedicine. The identification process is to insure that the correct individuals are anonymously engaged in patient - care giver transactions and information sharing.

Each care provider and patient whose identity is to be secured and authenticated is issued a tamper destructive information appliance 302. Preferably, the information appliance is a portable device such as a smart card. The smart cards store biometric/personal information for identification, and can also contain pertinent health or medical information concerning the patient stored within one or more of the segments of the string stored by the information appliance 302. Further, because the smart card 302 identifies the user, the user maintains possession and control over their own identifying and personal information, and that information is not broadcasted over any

Inventor: Dave Applebaum
Docket No. BAT 0039 PA / 12615 - 12753 - 13120
DRAFT DOCUMENT October 15, 2001

network. This process also "verifies" that the remote transaction being conducted is with who is being represented and that the individual is not being tricked into providing information to someone not intended.

5 Having described the invention in detail and by reference to preferred embodiments thereof, it will be apparent that modifications and variations are possible without departing from the scope of the invention defined in the appended claims.

What is claimed is:

10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200